REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1.   Restriction Requirement

In the previous Official Action, the Applicant provided a specific reason why the restriction requirement was improper, namely that examination of all of the claims could not possibly be a serious burden on the Examiner since the Examiner had already twice examined and (presumably) thoroughly searched all of the claims.

In reply, the election was treated without traverse, because "no burden" was not considered to be a reason for traversal. The Examiner is apparently unaware of the requirements for a proper restriction requirement, one of which in fact is that there by a burden on the Examiner. The MPEP does not permit an Examiner to arbitrarily restrict an application after the application has been examined and the Applicant has already responded twice to rejections of all the claims (none of which had merit), thereby greatly increasing the financial burden on the Applicant without a corresponding benefit to the Office. As explained in MPEP 803, part I:

> There are **two criteria** for a proper requirement for restriction between patentably distinct inventions:
> (A) The invention must be independent. . .or distinct as claimed; and
> (B) There would be a <u>serious burden</u> on the examiner if restriction is not required (emphasis added).

As explained in the immediately preceding paragraph of MPEP 803:

> If the search and examination of all the claims in an application can be made without serious burden, the examiner **must** examine them on the merits, even though they include claims to independent or distinct inventions.

It is respectfully submitted that since the Examiner had already examined both sets of claims on the merits, it would hardly be a burden to continue to examine essentially the <u>same</u> claims as were previously examined and searched.

10

Since "burden" on the Examiner is one of the two requirements for a restriction, and since the Applicant specifically pointed out the error in the restriction requirement, namely lack of burden (because the Examiner had already twice examined the claims subject to restriction on the merits), it is respectfully submitted that the election should not have been treated as being <u>without traverse.</u>

If necessary, the Applicant will petition the characterization of the election as being "without traverse," in order to preserve the right to petition against the restriction requirement itself. However, it would expedite prosecution of the application and save Patent Office resources if the Examiner would at least characterize the election as "with traverse" so that the requirement can be directly petitioned. Of course, the need for a petition could be eliminated altogether simply by withdrawing the restriction requirement, since the requirement is clearly wrong.

2.   <u>Rejection of Claims 28-30, 33, and 42 Under 35 USC §112, 2nd Paragraph</u>

This rejection has been addressed by amending claim 28 to positively recite "a memory" and "a data carrier."

In addition, claims 30 and 33 have been amended to clarify that the "combinations" recited therein are the respective combinations recited in claim 29 and claim 26.

Having addressed each of the grounds for rejection under 35 USC §112, 2nd Paragraph, withdrawal of the rejection is respectfully requested.

3.   <u>Rejection of Claims 26-32 and 42 Under 35 USC §102(e), and Rejection of Claim 33 Under 35 USC §103(a), in view of U.S. Patent No. 6,049,613 (Jakobsson)</u>

These rejections are respectfully traversed on the grounds that the Jakobsson patent fails to disclose or suggest a data carrier, as claimed, in which operating program commands are arranged to prevent signals caused by execution of the commands from being used to infer data being processed. Instead, the Jakobsson patent is concerned with parallel encryption of

permutations to insure that "no processor cheated, no processor made a mistake, and no error was otherwise introduced." Permutation and parallel encryption of *data* is not the same as concealing the *operations* that carry out the permutation and parallel encryption of data, and in particular is not the same as concealing the permutation and/or encryption operations from detection via signal emission.

It does no good to encrypt data, as taught by Jakobsson, if the operations used to detect the data can be inferred from signal emissions. Jakobsson's method is only useful insofar as the signal emissions that occur during processing are not subject to interception. Jakobsson is concerned with <u>data</u> protection, but is not at all concerned with data inference by interception of signal emissions that occur during the data protection, and takes <u>no</u> steps to prevent such inference. The present invention, on the other hand, applies to the situation where signal emissions are vulnerable to interception, such as might occur in connection with a public card reader of an ATM.

Claim 1 of the present application specifically requires that the operating program commands either be selected or executed in such a way that *"data processed with the corresponding program commands* **cannot be inferred** *from said signals that are caused by execution of said commands,"* the signals being positively recited as being *"detected <u>outside</u> the semiconductor chip."* Jakobsson is not at all concerned with signals detected <u>outside</u> the semiconductor chip, or with the preventing someone from inferring data being processed based on interception of the signals.

In the Official Action, the Examiner alleges that *"Jakobsson discloses a method of protecting secret data, where the method includes falsifying input data by combination with auxiliary data. . ., and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data, where the auxiliary value was previously determined. . .."* Thus, the rejection is based solely on Jakobsson's teaching of input data falsification. However, the claimed invention is **not** data falsification. **The Examiner has based**

the rejection on features that are <u>not</u> even claimed, while <u>ignoring</u> what is actually claimed, namely arranging <u>operating program commands</u> in such a way that the data is not detectable from outside the chip.

The invention does not seek to falsify input data, although it can be used to protect input data falsification operations. Instead, the invention is concerned with the problem of inferring the data by detecting what is being done to the data. It does no good to falsify the data if the falsification steps can be determined by intercepting signals generated by the falsification steps. In order for the falsification to be successful in that situation, one must take the additional step of making sure that the falsification steps cannot be monitored based on signals emitted thereby.

In the discussion of claim 26, the Examiner cites col. 5, line 56 to col. 6, line 42, and col. 6, line 56 to col. 7, line 3 of the Jakobsson patent. These passages describe an encryption process that involves data permutation or blinding (as part of Jakobsson's overall teachings concerning parallel processing) so that one cannot discover the input by analyzing the output. However, Jakobsson is not concerned, either implicitly or explicitly, with the possibility that not only the output, but the entire encryption process may be detected by monitoring signal emissions. <u>Data blinding is useless if the steps used in data blinding can be observed</u>. In many situations, the encryption process itself is secure, in which case Jakobsson's data blinding or encryption processes may be useful. Data blinding and encryption are not useful, however, in situations where the data blinding and encryption process can itself be observed via signal emissions from the chip that carries out the data blinding and/or encryption.

Essentially, in making the rejection, the Examiner has paraphrased the claim language and, in doing so, ignored a number of specific claim limitations, including the positive recitation of

-    **operating program commands that cause signal emissions detectable outside a chip and**

-    selection or execution of the **operating program commands** in such as way that *"the operating program commands cannot be inferred from said signals that are caused by*

> *execution of said commands and that have been detected <u>outside</u> the semiconductor chip.*"
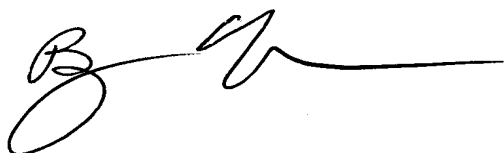
The Jakobsson patent simply does <u>not</u> disclose or suggest these limitations. Data blinding and encryption as taught by Jakobsson, and likely numerous other references, is not concerned with signal emission caused by execution of operating program commands.

Since the Jakobsson patent, whether considered individually or in reasonable combination with any of the references of record, does not disclose or suggest selection or execution of operating program command to prevent detection of data based on <u>signal emissions</u> resulting from program execution, it is respectfully submitted that the Jakobsson patent cannot anticipate and does not suggest the claimed invention, and therefore withdrawal of the rejections under 35 USC §§102(e) and 103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: May 8, 2006

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\beu\Pending Q...Z\V\VATER 700656\a03.wpd

14